STANDING OPERATING
PROCEDURE
NO. TBO- 01-01

Directorate of Public Works
HQ, III CORPS AND FORT HOOD
FORT HOOD, TEXAS

INFORMATION SYSTEMS SECURITY
PROCESSING UNCLASSIFIED INFORMATION
JULY 2001

I . REFERENCE. AR 380-19, Information Systems Security, 27 Feb 98.

2. PURPOSE. This SOP sets forth the operating procedures, to be followed by each individual user of a computer system, for the protection of software and information stored on or derived from each system within the Directorate of Public Works (DPW) area of responsibility.

3- RESPONSIBILITY. Each user/operator of a computer within the organization will be responsible for the protection of all software and information stored on or generated by the computer, in accordance with present guidelines and regulations. Each user/operator will ensure that the computer is operated and maintained in accordance with this Standard Operating Procedure, AR 380-19 and as recommended by the manufacturer. Any changes or additions to this Standard Operating Procedures will be forwarded to Information Assurance Security Officer (IASO).

4. APPLICABILITY. This Standard Operating Procedure applies to all computer systems located and supported by DPW and all software and information stored or generated by each computer system in the directorate. It is applicable to all personnel utilizing equipment and software.

5. ACCOUNTABILITY. All personnel having access to computer systems will be held accountable for his or her actions on the system. This includes reviewing and complying with software licensing agreements.

6. ACCESS. No individual will be granted access to the computer system without the approval of the System Administrator (SA) or Information Assurance Security Officer (1ASO) . Access to the computer is limited to only personnel who are assigned to the section, have the appropriate security investigation and have the "need-to-know".

7. SECURITY TRAINING AND AWARENESS. All personnel operating computer systems will be briefed prior to operating a computer on all security requirements by the system SA or IASO with special emphasis being placed on requirements unique to the information they handle. This briefing will be in accordance with AR 380-19, paragraph 2-16 and Annex B.

a. Supervisors of personnel operating computer systems equipment will be sensitive to changes in conduct and/or in personality of the operator/user, and will report any adverse changes to the IASO or SA.

b. Security Briefings:

(1) Security briefings will be provided to all personnel who will operate computer equipment in accordance with AR 380-19 Paragraph 2-16 and Annex B.

(2) The briefings will be orientated toward the local security environment and the computer equipment and software.

(3) No security related questions will go unanswered and no one will begin his/her duties without knowing and understanding what is expected.

8. PHYSICAL CONTROLS. All hardware, software, documentation, and all sensitive data handled by the computer system will be protected to prevent unauthorized disclosure, destruction, or modification in accordance with AR 380-19 and AR 380-5. The following controls will apply:

a. When leaving the office containing a computer system the user will either log off or ensure the computer has a password protected screen saver. The password must be a minimum of eight characters and a combination of letters, numbers and symbols. Unless an operational requirement exits for a computer to remain on at all times, users will log off the computer at the end of the work day. The windows and doors will be locked, and checked by the office personnel at the end of the business day.

b. When unassigned personnel visit the office; they will be monitored to guard against unauthorized access to the organization's computer systems.

c. All software will be stored in a diskette file box, which will be placed in a locked container/cabinet in a separate location from the back-up diskettes. This will enable the detection of signs of tampering.

d. No computer system, which includes all associated hardware, will be disassembled, moved or otherwise altered unless authorized by the IMO and IASO.

9. MARKING. All media will be marked and protected commensurate with the requirements for the highest level of sensitivity and most restrictive category of information stored on the media.

10. LEAST PRIVILEGE. No person will have access to the computer based upon his or her rank or position. All personnel in the section will have the proper clearance, access, and need to know for all information stored on the computer as verified by the IASO.

11. DATA CONTINUITY. IASO will ensure that all software is marked to reflect the owner and proponent of the software to reflect the author of the program.

12. DATA INTEGRITY. IASO will ensure that all data is stored in a proper manner and the anti-viral program is installed on all assigned computer systems. All personnel will be trained on the proper use of the program.

13. CONTINGENCY PLANNING. To provide for backup in the event of a disaster. Attach copy of contingency plan or describe below.

14. ACCREDITATION. Before operation of the system the IASO will ensure that all computer systems have been accredited and will submit the re-accreditation request three months prior to current accreditation expiration.

15. SOFTWARE SECURITY. Only software that has been specifically developed or approved for use, **or** has been purchased or leased by an authorized U.S. Government representative, will be used on any government owned computer system. A backup copy of all software will be made and stored in a locked container/cabinet. Original program software will be stored in a locked container away from the computer. The IMO will maintain site licenses in a locked container/cabinet. Upon receipt of commercial software the IMO or SA will register the software with the manufacturer by mailing in the registration card.

16. SECURITY PLANNING. IASO will enforce guidelines and procedures outlined in this Standard Operating Procedure and the Accreditation Document.

17. RISK MANAGEMENT.

a. General factors. The computer systems are located in building(s) of the Activity/Directorate. All personnel using these systems will have the appropriate security clearance or investigation for the automated data processing level and need-to-know for the operating mode of the computer system. The IASO will verify the investigation or the security clearance required. Countermeasures have been implemented to combat each threat. An ongoing assessment will be made by the IASO and each computer operator to check effectiveness of implemented countermeasures. The 1ASO will notify Installation Information Assurance Manager of any changes in their local threat posture.

b. Foreign intelligence service.

(1) The computer system will process Unclassified But Sensitive (UBS) information therefore the system is considered a potential target of the foreign intelligence service.

(2) Risk assessment: Minimal to Moderate

(3) Countermeasures: Each individual will have a background check and access should be based on "need-to-know" requirements. Each individual will receive an annual SAEDA brief. Only personnel working in the section should have access to the computers, unless granted access by the IASO or SA. The system will be monitored during duty hours by all section personnel and secured by a locked barrier during non-duty hours. The laptop computers will be stored at the end of the duty day in a locked container/cabinet/desks in accordance with AR 380-19.

c. Man-made or natural disaster.

(1) The AIS is subject to damage or destruction by fire, smoke, heat and power surges.

(2) Risk assessment: Minimal with the exception of power surges.

(3) Countermeasures: A non-water fire extinguisher will be easily accessible. Surge protectors will be used at all times. There is no smoking allowed in the office area and the temperature of the room containing the computers will be kept at a moderate level.

d.. Deliberate or inadvertent error.

(1) Systems software can be damaged or erased through careless behavior, untrained personnel, and intentionally.

(2) Risk assessment: Minimal to Moderate

(3) Countermeasures: All personnel will be briefed by the IASO or SA on proper operating procedures and rules prior to initial operation of the system. There will be no eating or drinking in the vicinity of the computer system. All unclassified software will be stored, while not in use, in a filing cabinet enabling the detection of tampering. anti-viral software will be installed on all computers and will be used to check all diskettes before they are used in the computer. All assigned personnel will be trained on the proper use of the software. The IASO or SA oversees generation, issuance, and control of all passwords.

18. OTHER CONSIDERATIONS.

a. Environmental Protections. Each user will adhere to the following guidelines.

(1) At the end of each working day the computer system and the area around it will be dusted and cleaned properly, to decrease the risk of a mechanical malfunction of the computer system

(2) Use caution while eating in close proximity to the computer and. only covered drink containers are authorized within three feet of the computer system. Smoking is prohibited within the building.

(3) Do not expose the computer system to direct sunlight or place it in close proximity to heaters or radiators.

(4) Keep the heat in the room containing the computer system at a moderate level.

(5) Do not place the computer system near any electromagnetic devices.

(6) Avoid placing unnecessary metal objects near the computer system.

(7) Connect the computer to a separate circuit if possible. Avoid outlets on the same circuit with large appliances/machines.

(8) Make sure every component of the system is grounded with three pronged plugs.

(9) All computer equipment should be labeled as US Government Property.

(10) Keep all cables out of the way so they will not be stepped on, tripped over or pulled loose during work sessions.

(11) AR 25-1, Chapter 5, contains policy on the approval to use privately (employee) owned computers. Employee owned computers are not authorized on the Installation for administrative or operational use in an organization, unless approved by the Director of Information Management and accredited. All applications should be forwarded through the Installation Information Assurance Manager.

b. Removable Diskettes and CD ROMs. Each user will adhere to the following guidelines.

(1) Put the diskettes or CD ROMs in protective jackets when not in use.

(2) Keep diskettes or CD ROMs away from heat sources, electrical, and magnetic devices.

(3) Never bend or write on diskettes or CD ROMs.

(4) Never touch the exposed recording surfaces of the diskettes.

(5) Make backup diskettes of data generated.

(6) Always write protect original diskettes.

(7) Always SCAN FOR VIRUSES ON ANY NEW SYSTEM AND ON ALL DISKETTES or CD ROMs prior to use.

c. Mandatory Reporting Requirements (AR380-19, para. 2-27a).

(1) Unexplainable output received at a terminal.

(2) Inconsistent or incomplete security marking on output, extraneous data included in output, or failure to protect output properly.

(3) Abnormal system response.

(4) Any indication of an unauthorized user attempting to access the system, including unexplained attempts to log-on unsuccessfully from a remote terminal.

(5) Any indication of unexplained modification of files or unregistered, abnormal "writes" to media.

(6) Any indication of a virus includes the name if captured by anti-viral program.

d. User's Antiviral Response to a Virus Infection.

(1) Write down or print any message on the computer screen, to include abbreviations or acronyms.

(2) Shut the system down immediately after copying the data.

(3) Report virus infection to your IASO or SA who in turn will report it to the DOIM Help Desk.

(4) Control all media associated with the computer.

(5) Do not let anyone use the computer until it has been cleared by your SA.

(6) Scan all associated media with anti viral program before returning back into the inventory of available applications.

19. Lap Top Computers

(1) Laptops used for processing SBU information will be marked with SF 710 "Unclassified" on the keyboard side of the computer.

(2) Laptops used for designated SBU processing under the provisions of this policy will not be connected to any computer while the system is processing classified information.

(3) Documentation requirements (e.g., use of property passes, hand receipts and MOAS,) prior to removal of the equipment and software from the activity/installation.

(4) Laptop or other portable computers, regardless of the classification of the data processed, will not be allowed in and out of a SCIF and should not be procured/obtained for that environment when the operational mission requires automation support for an individual or official travel, prior arrangements should be made with the site(s) he/she is visiting for the required support. For collateral information processing capability available at the visited SCIF(s) so that only software/data is transported..

(5) Security inspections and anti-virus up dates: It is the Users responsibility to ensure the Laptop has the most current version of anti-virus.

(6) Laptop will use only TSACS for remote dial into the network

(7) Laptops users are to follow same security procedures as workstations.

DAVID C. WRBAS
Deputy Director of Public Works